THE CLAIMS

A detailed listing of all of originally filed Claims 1–36 is provided below. A status identifier is provided for each claim in a parenthetical expression following each claim number.

1.   (Currently Amended) A method of providing a mobile computing machine with privileged access to a computing resource, the method comprising the steps of:

obtaining a certificate credentials with a unique machine identifier to facilitate authenticating an identity of the mobile computing unit;

providing the certificate credentials to an authenticator to prove the machine identity, the authenticator controlling access to the computing resource; and

establishing access to the computing resource using authorization information obtained from the authenticator to reflect a relative security level credentials for a user of the mobile computing unit, the authorization information corresponding to the authenticated identity of the mobile computing unit.

2.   (Original)   The method of claim 1 wherein the mobile computing unit communicates with the computing resource using at least one wireless link.

3.   (Original)   The method of claim 1 wherein the authorization information includes a key for encrypting communications from the mobile computing unit to an input port.

4.   (Original)   The method of claim 3 wherein the key is a symmetric session key.

5.   (Previously Presented) The method of claim 1 further comprising, prior to the obtaining step, comprising detecting a failure of a user of the mobile computing unit to complete a logon to access the computing resource.

6.   (Previously Presented) The method of claim 1 further comprising, prior to the obtaining step, determining that the mobile computing unit does not have a certificate to prove machine identity.

7.   (Original)   The method of claim 1 further comprising the step of storing the unique machine identifier on the mobile computing unit for subsequent use.

8.   (Original)   The method of claim 1 further comprising the step of storing the certificate on the mobile computing unit.

9.   (Original)   The method of claim 1 further comprising the step of receiving the unique machine identifier.

10.   (Original)   The method of claim 1 further comprising the steps of obtaining by the domain controller the certificate from a certificate authority; and receiving the certificate from a domain controller.

11.   (Original)   The method of claim 10 wherein the certificate is obtained by the domain controller in response to a user request from a user, the user using the mobile computing unit to access the computing resource.

12 – 15.   (Canceled)

16.   (Currently Amended) A method of providing a user secure access to a computing resource from an external site, the method comprising the steps of:

sending a request to access a computing resource;

providing a user identifier, the user identifier corresponding to an asserted identity, to a proxy authenticating server via a remote access point;

providing, in response to a challenge, ~~a certificate~~ credentials to authenticate the asserted identity, to the proxy authenticating server via the remote access point; and

receiving an address for sending and receiving data to and from the computing resource, the address corresponding to limited access to the computing resource based on the asserted identity.

17.   (Original)   The method of claim 16 wherein the address for sending and receiving data is a universal resource locator.

18.   (Original)   The method of claim 17 further comprising receiving by the user a key for encrypting communications to the computing resource.

19.   (Original)   The method of claim 18 further comprising using the key to decrypt communications from the computing resource.

20.   (Previously Presented) A method for setting up a secure link between a server and a client using wireless transmission, wherein the client machine is a wireless station and the server is an authenticator, the client and server securely exchanging keys to establish the secure link with encryption of at least one message exchanged between the client and the server, the method comprising the steps of:

asserting an identity;

responding to an authentication request by providing ~~a certificate~~ <u>credentials</u> to prove the asserted identity; and

generating an initial encryption key for encrypting communications over the secure link from the information in the certificate based on a relative security level accorded to the asserted identity.

21.   (Currently Amended) A computer-readable medium having computer executable instructions for performing the steps of a method of providing a machine with privileged access to a computing resource, the method comprising the steps of:

obtaining ~~a certificate~~ <u>credentials</u> with a unique machine identifier to facilitate authenticating an identity of the mobile computing unit;

providing the ~~certificate~~ <u>credentials</u> to an authenticator to prove the machine identity, the authenticator controlling access to the computing resource; and

establishing access to the computing resource using authorization information obtained from the authenticator to reflect ~~a relative security level~~ <u>credentials</u> for a user of the mobile computing unit, the authorization information corresponding to the authenticated identity of the mobile computing unit.

22.   (Original)   A computer-readable medium as in claim 21, having computer executable instructions for performing the step of using the machine identity is conditional on the failure of a user on the machine to complete a log-in to access the computing resource.

23.   (Original)   A computer-readable medium as in claim 21 having computer executable instructions wherein the mobile computing unit communicates with the computing resource using at least one wireless link.

24.   (Original)   A computer-readable medium as in claim 21 having computer executable instructions wherein the authorization information includes a key for encrypting communications from the mobile computing unit to an input port.

25.   (Original)   A computer-readable medium as in claim 21, having computer executable instructions for performing the additional step of storing the unique machine identifier on the mobile computing unit for subsequent use.

26.   (Original)   A computer-readable medium as in claim 21, having computer executable instructions for performing the additional step of storing the certificate on the mobile computing unit.

27.   (Original)   A computer-readable medium as in claim 21, having computer executable instructions for performing the additional steps of obtaining, by the domain controller, the certificate from a certificate authority; and receiving the certificate from the domain controller.

28.   (Original)   A computer-readable medium as in claim 27 having computer executable instructions wherein the certificate is obtained by the domain controller in response to a user-request from a user to use a computing resource.

29 - 32.   (Canceled)

33.   (Currently Amended) A computer-readable medium having computer executable instructions for performing the steps of a method of providing a user secure access to a computing resource from an external site, the method comprising the steps of:

sending a request to access a computing resource;

providing a user identifier, the user identifier corresponding to an asserted identity, to initiate a log-in in order to access the computing resource;

providing, in response to a challenge, a certificate credentials to authenticate the asserted identity to obtain access to the computing resource; and

receiving an address for sending and receiving data to and from the computing resource based on the asserted identity.

34.   (Original)   A computer-readable medium as in claim 33 having computer executable instructions wherein the address for sending and receiving data is a universal resource locator.

35.   (Original)   A computer-readable medium as in claim 34 having computer executable instructions for performing the step of receiving a key for encrypting communications to the computing resource.

36.   (Original)   A computer-readable medium as in claim 35 having computer executable instructions for performing the step of using the key to decrypt communications from the computing resource.